REMARKS/ARGUMENTS

Favorable reconsideration of this application is respectfully requested.

With respect to the objection in paragraph 3 of the Office Action, applicants believe there is nothing improper by referring to the web page "http://www.bluetooth.com" in the specification, and applicants have not seen any prohibition against such a recitation at M.P.E.P. § 608.01. Applicants believe that notation in the specification at page 12, line 13 provides relevant information and thus is proper.

The specification is amended by the present response to correct a minor grammatical informality.

Claims 1-24 are pending in this application. Claims 23 and 24 are added by the present response, and are believed to be clearly supported for example by the original claims. Claims 1-22 were rejected under 35 U.S.C. § 103(a) as unpatentable over "Bluetooth Specification", Bluetooth Security, November 29, 1999, pages 149-178 (herein "Bluetooth") in view of "5C Digital Transmission Content Protection White Paper", Revision 1.0, July 14, 1998, pages 1-13 (herein "5C White Paper").

Addressing the above-noted rejected, that rejection is traversed by the present response.

Applicants respectfully submit the claims as currently written distinguish over the applied art, and respectfully submit the combination of teachings in the Bluetooth reference and the 5C White Paper do not fully meet all the claim limitations. Specifically, the claims set forth how first and second encryption keys are utilized to transmit copy protected contents data securely, and such specific combined usage of the first and second encryption keys is not believed to be taught or suggested by the combination of teachings in the Bluetooth reference and the 5C White Paper.

One objective of the present invention is to provide enhanced transfer of copyright protected contents data, and to particularly realize a secure copyright protection even in a radio network environment.[1]

With reference to Fig. 1 in the present specification as a non-limiting example, the present invention can be applied to a radio communication system including a portable MPEG4 player 101 and a portable viewer 102, which are both owned by the same person and thus that are authorized to communicate information with each other. The portable MPEG4 player 101 and the portable viewer 102 are located within an area in which a connection by a local area radio network is possible. Further, another portable viewer 103 owned by a different entity may also enter that local area, but the claimed system prevents that other portable viewer 103 from viewing data from the portable MPEG4 player 101 as the other portable viewer 103 is owned by a different entity and does not have authorization to view data provided from the portable MPEG4 player 101.

The claimed invention utilizes a specific sequence of communication between the MPEG4 player 101 and the portable viewer 102 to assure secure communication and to ensure that the portable viewer 103 cannot view data from the portable MPEG4 player 101. As discussed in the present specification at page 20, line 1 to page 21, line 31 and with respect to Fig. 5 in the present specification, such a sequence of communicating between the MPEG4 player 101 and the portable viewer 102 is carried out as follows:

(1) a Bluetooth layer link key sharing procedure is carried out (step S13) when PIN code values on both devices coincide;

(2) a value of a link key K1 to be used in a subsequent authentication and key exchange is shared (steps S14 and S15);

[1] See for example the present specification at page 3, lines 3-6.

(3) a Bluetooth layer authentication procedure and a Bluetooth layer key exchange procedure are carried out (steps S16 and S17);

(4) a value of a Bluetooth first encryption key (layer encryption key Kbt) is shared (steps S18 and S19);

(5) a DTCP authentication and key exchange are carried out by utilizing a Bluetooth layer level encryption (step S20);

(6) a value of a second encryption key (second encryption key Kc) is shared on a DTCP layer (copyright protection layer) (steps S21 and S22);

(7) the portable MPEG4 player 101 transmits contents (MPEG4 data) to be transmitted by encrypting them by using the second encryption key Kc, to the portable viewer 102 (steps S23 and S24); and

(8) the portable viewer 102 decrypts the received encrypted contents by using the DTCP level second encryption key Kc (step S25).

Another transferring sequence between the portable MPEG4 player 101 and the portable viewer 102 can be carried out according to the following processes (as noted in the present specification at page 25 lines 7-25 and Fig. 9);

(1) the portable MPEG4 player 101 encrypts the contents (MPEG4 data) to be transmitted by using the encryption key first, and then encrypts the copyright protected contents by using the encryption key Kbt (step S54); and

(2) the portable viewer 102 decrypts the received encrypted contents by using the encryption key Kbt first, and then the decrypted contents by using the encryption key Kc (step S54).

Thus, according to the present invention, it is possible to share the encryption key properly only between the legitimate devices that can successfully complete the

authentication procedure, so that it becomes possible to realize the data transfer using the cipher communication only between devices that have properly shared the encryption key.

Applicants respectfully submit the Bluetooth reference and the 5C White Paper do not teach or suggest how first and second encryption keys can be combined as claimed to transmit copy protected contents data securely.

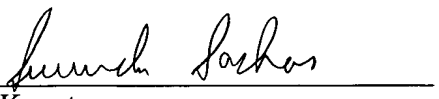
In the claims a first key exchange unit generates a first encryption key and shares the first encryption key with the receiving device. Then, a second authentification unit carries out a second authentification to protect copyrights of contents data using the first encryption key. Neither the Bluetooth nor the 5C White Paper reference teaches or suggests a second authentification unit performing such an operation based on utilizing a first encryption key. Then, in the claimed invention a second key exchange is executed and contents are then transmitted utilizing the second encryption key. Neither the Bluetooth reference nor the 5C White Paper teach or suggest such features. The claims set forth a combined usage of first and second encryption keys as discussed above that are neither taught nor suggested by the applied art.

In such ways, the claims as currently written are believed to clearly distinguish over the applied Bluetooth reference in view of the 5C White Paper.

As no other issues are pending in this application, it is respectfully submitted that the present application is now in condition for allowance, and it is hereby respectfully requested that this case be passed to issue.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Customer Number
22850

Eckhard H. Kuesters
Registration No. 28,870

Surinder Sachar
Registration No. 34,423
Attorneys of Record

Tel: (703) 413-3000
Fax: (703) 413 -2220
EHK/SNS:sjh

I:\ATTY\SNS\21's\213200\213200US-AM.DOC